In the Claims:

Following is a complete listing of the claims pending in the application, as amended:

1. – 139. (Cancelled)

140. (New) A method performed by a server of a public key system, said public key system further comprising a plurality of client terminals, said method comprising the steps of:
   storing a first list of fingerprints of digitally encoded data;
   computing a first fingerprint for at least a part of said list of fingerprints; and
   providing said computed first fingerprint.

141. (New) The method according to claim 140, wherein said step of computing said first fingerprint comprises the steps of:
   obtaining one or more entries of said first list of fingerprints, whereby said one or more entries are to be covered by said first fingerprint; and
   computing a hash value on at least said obtained one or more entries.

142. (New) The method according to claim 140, wherein said first list of fingerprints further comprises at least one of the following:
   a unique identifier associated with each fingerprint;
   a time specification associated with each fingerprint, whereby said time specification specifies at least one of a time of entry into said first list associated with said fingerprint or said digital data, a time of generation of said fingerprint or said digital data, or a time of provision of said fingerprint or said digital data to said server; or
   a link to digital data or an association with digital data of each fingerprint.

143. (New) The method according to claim 141, wherein said one or more entries in said step of obtaining said computed first fingerprint further comprising at least one of a unique identifier or a time specification associated with a fingerprint.

144. (New) The method according to claim 142, wherein said unique identifier, said time specification, said link or said association are established and assigned by said server as part of said storing step.

145. (New) The method according to claim 140, wherein said step of providing said computed first fingerprint comprises attaching said first fingerprint to a message that is sent to at least one of said plurality of user terminals.

146. (New) The method according to claim 140, wherein said step of providing said computed first fingerprint or said step of computing said first fingerprint further comprises signing said first fingerprint by said server.

147. (New) The method according to claim 140, wherein said step of storing a first list of fingerprints comprises the steps of:
    receiving digital data;
    establishing at least one of the integrity of said digital data, the identity of a sender of said digital data and the authenticity of said sender; whereby said establishing comprises at least one of verifying a digital signature for said digital data, verifying a fingerprint associated with said digital data or sender, using a secure and trusted connection for the communication with said sender, and applying an encryption scheme for the said received digital data;
    computing a hash value on at least said digital data; and
    adding said hash value to said first list of fingerprints.

148. (New) The method according to claim 140, wherein at least said steps of computing a first fingerprint and providing said computed first fingerprint are performed repeatedly according to a timed schedule, and wherein said first list of fingerprints can be augmented or continued with further entries.

149. (New) The method according to claim 148, wherein said step of providing said computed first fingerprint comprises providing or updating said first fingerprint on an hourly, daily, weekly, monthly or another regular time period basis.

150. (New) The method according to claim 140, wherein said step of providing said computed first fingerprint further comprises associating and providing at least one of a time specification, a validity period information or another identifier providing for establishing the validity of said provisioned first fingerprint.

151. (New) A method performed by a client terminal of a public key system, said public key system comprising a plurality of client terminals and at least one server, said method comprising the steps of:
    obtaining a first list of fingerprints of digitally encoded data from a first source;
    obtaining a first fingerprint of said list of fingerprints from a first source;
    obtaining a second fingerprint of said list of fingerprints from a second source; and
    comparing said first and said second fingerprint.

152. (New) The method according to claim 151, further comprising the steps of:
    computing a fingerprint of said obtained first list of fingerprints;
    comparing said computed fingerprint and said obtained first and second fingerprints;
    if at least one of said comparing steps result in different fingerprints, establishing that the data integrity of said received fingerprints or said first list of fingerprints has been compromised;

153.   (New) The method according to claim 151, further comprising the steps of:

obtaining at least one of said digitally encoded data of said fingerprint list;

computing a fingerprint of said obtained digital data;

comparing said computed fingerprint with the fingerprint for said obtained digital
      data in said received list of fingerprints; and

if said comparing step results in different fingerprints, establishing that the data
      integrity of said received digital data or said list of fingerprints has been
      compromised;

154.   (New) The method according to claim 151, further comprising at least one of:

verifying a digital signature for said received first and second fingerprint;

verifying a digital signature for a received list of fingerprints;

verifying a fingerprint associated with said received first and second fingerprint or
      said first and second source; and

receiving a user input to perform at least one of said steps of verifying a digital
      signature and verifying a fingerprint.

155.   (New) The method according to claim 151, wherein said steps of obtaining
said first and second fingerprint comprising a step of

      receiving said first and second fingerprint together with a message sent to said
            client terminal via communications media of a public network connecting said
            client terminals and said server; and

      said method further comprising a step of:

            attaching a fingerprint of said list of fingerprints to a message sent to another
                  client terminal via said communications media of a public network
                  connecting said client terminals.

156.   (New) The method according to claim 155, wherein said steps of obtaining
said first and second fingerprint and attaching a fingerprint are accomplished automatically

without an explicit request by the receiving client terminal of said message but as part of a regular communication between client terminals not established for the purpose of exchanging said first or second fingerprint.

157. (New) The method according to claim 151, wherein said step of attaching a fingerprint further comprises associating and attaching at least one of a time specification, a validity period information or another identifier providing for establishing the validity of said provisioned fingerprint.

158. (New) The method according to claim 155, wherein said step of attaching a fingerprint to a message is only performed for fingerprints that are verified by said client terminal to be valid and authentic; whereby said verification may depend on the number of successful comparing steps that were performed for said attached fingerprint with received corresponding fingerprints of mutually different and/or independent sources; and wherein said step of attaching a fingerprint further comprises signing said fingerprint by said client terminal using a private key of said client terminal.

159. (New) The method according to claim 151, wherein said steps of obtaining said first and second fingerprint comprising a step of

determining whether a received fingerprint and/or a received list of fingerprints is valid and represents the latest published version by means of associated or attached information to said received fingerprint and/or received list of fingerprints or by means of a predetermined timed schedule known to said client terminal; and

if said received fingerprint and/or a received list of fingerprints is not valid, disregarding said received fingerprint and/or received list of fingerprints or requesting a fingerprint and/or a list of fingerprints from another source to replace the invalid versions.

160. (New) The method according to claim 151, wherein said client terminal further keeps and updates a record of received first and second fingerprints from different sources, whereby said record may comprise identifiers of the source of each fingerprint and whereby said updating may comprise removing a fingerprint from said record after having established that said fingerprint is invalid or said fingerprint or the respective source of said fingerprint cannot be trusted or successfully authenticated.

161. (New) The method according to claim 152, wherein said client terminal reports to at least one of said system, said server, a certificate authority of said system and a user of said client terminal in case said client terminal determines that the data integrity of said received fingerprints or said list of fingerprints has been compromised, whereby said reporting may comprise identifying and reporting the source of said compromised fingerprints or list.

162. (New) The method according to claim 141, wherein said step of obtaining one or more entries of said first list of fingerprints comprises obtaining a specific segment of entries of said first list of fingerprints, and wherein said step of computing said first fingerprint further comprises the steps of:

storing said computed hash value in a second list of fingerprints;

obtaining one or more entries of said second list of fingerprints in the same manner as said step of obtaining one or more entries of said first list, whereby said one or more entries are to be covered by said first fingerprint; and

computing a hash value on at least said obtained one or more entries of said second list of fingerprints in the same manner as said first step of computing a hash value.

163. (New) The method according to claim 162, wherein said specific segment is defined by a time interval, whereby said time specification of said obtained entries in said first list of fingerprints are associated with or covered by said time interval.

164. (New) The method according to claim 162, wherein said step of obtaining one or more entries of said second list of fingerprints comprises obtaining a specific segment of said second list of fingerprints, and wherein said step of computing said second fingerprint further comprises the steps of:

storing said computed hash value in a third list of fingerprints; and

obtaining one or more entries of said third list of fingerprints in the same manner as said step of obtaining one or more entries of said first list, whereby said one or more entries are to be covered by said first fingerprint; and

computing a hash value on at least said obtained one or more entries of said third list of fingerprints in the same manner as said first step of computing a hash value including optional steps of storing said hash value in a further list of fingerprints and subsequently computing a further hash value covering entries of said further list.

165. (New) The method according to claim 162, wherein said server provides said second list, said third list, said specific segment, a particular entry of said first, said second or said third list and/or a particular entry of a segment to another client terminal or to another party of said system, whereby said another client terminal or party has requested said provision.

166. (New) The method according to claim 165, wherein said server receives a request specifying at least one of: a time interval, a specific fingerprint of one of said lists of fingerprints and the respective digital data to said specific fingerprint.

167. (New) The method according to claim 162, wherein several second and several third lists of fingerprints and respectively several second and third fingerprints of said fingerprint lists are computed and/or provided, whereby each list may be used for different kinds of digital data, according to different time schedules and time intervals, and/or according to different maximum numbers of entries in each list.

168.   (New)   The method according to claim 162, wherein said second list of fingerprints is said first list of fingerprints or a specific segment of said first list of fingerprints.

169.   (New)   The method according to claim 167, wherein said different time schedules, different time intervals or said different maximum numbers of entries are adapted or specified by said server or a dedicated means of said system according to payload and performance specifications for at least one of said system, said server and said client terminals.

170.   (New)   The method according to claim 162, wherein said computed fingerprints of at least one of said first list of fingerprints, said second list of fingerprints or said first fingerprint can be further added to at least one of said specific segment of said first list, another segment of said first list, another first list, said second list, another second list, said third list, another third list, or a further list of fingerprints compiled from entries of said lists.

171.   (New)   The method according to claim 162, wherein one or more entries of said segment, said first list, said second list, and/or said third list are added to at least one of said specific segment of said first list, another segment of said first list, another first list, said second list, another second list, said third list, another third list, or a further list of fingerprints compiled from entries of said lists.

172.   (New)   The method according to claim 151, further comprising the steps of:
obtaining digital data;
requesting a second list of fingerprints, whereby said second list of fingerprints
        comprises fingerprint entries that are to be used for computing at least one of
        the fingerprints in said first list of fingerprints, and whereby at least one of
        said fingerprint entries covers said obtained digital data;

obtaining said requested second list of fingerprints;

computing a first hash value on the fingerprint entries of said second list that are to be used for computing a specific fingerprint in said first list of fingerprints, whereby at least one of said fingerprint entries covers said obtained digital data and whereby said specific fingerprint therefore covers said obtained digital data;

comparing said computed first hash value with said specific fingerprint;

if said comparing step results in different fingerprints, establishing that the data integrity of said obtained digital data or at least one of said lists of fingerprints has been compromised;

computing a second hash value for said obtained digital data;

comparing said computed second hash value with the fingerprint in said second list of fingerprints that covers said obtained digital data; and

if said comparing step results in different fingerprints, establishing that the data integrity of said obtained digital data or at least one of said lists of fingerprints has been compromised.

173.   (New) The method according to claim 172, wherein said step of computing a second hash value for said obtained digital data comprises the steps of:

requesting a third list of fingerprints, whereby said third list of fingerprints comprises fingerprint entries that are to be used for computing at least one of the fingerprints in said second list of fingerprints, and whereby at least one of said fingerprint entries covers said obtained digital data;

obtaining said requested third list of fingerprints;

computing a third hash value on the fingerprint entries of said third list that are to be used for computing a specific fingerprint in said second list of fingerprints, whereby at least one of said fingerprint entries in said third list of fingerprints covers said obtained digital data;

comparing said computed third hash value with said specific fingerprint in said second list of fingerprints;

if said comparing step results in different fingerprints, establishing that the data integrity of said obtained digital data or at least one of said lists of fingerprints has been compromised.

174. (New) The method according to claim 172, wherein at least one of said first, said second or said third list of fingerprints is a segment of another list of fingerprints.

175. (New) The method according to one of claim 172, wherein said steps of requesting a list of fingerprints comprising a step of specifying said requested list of fingerprints by specifying at least one of:

a time interval associated with the entries of said requested list,

a time specification for at least one entry of said requested list,

at least one fingerprint of said requested list;

at least one digital data covered by at least fingerprint of said requested list,

an identifier for said requested list, and

an identifier for at least one entry of said requested list.

176. (New) The method according to claim 140, wherein said digital data is comprised of at least one of: a public key of a public key pair, a certificate, a computer program, a software file, a database, an executable file, a digital picture, video or audio information and a data file.

177. (New) A computer-readable storage medium having a computer program for controlling a plurality of client terminals to participate in and perform operations according to a method as specified by claim 151.

178. (New) A computer-readable storage medium having a computer program for controlling a server to participate in and perform operations according to a method as specified by claim 140.

179. (New) A method for providing for a secure distribution of digital data in a public key system, the method comprising:

encrypting digital data using a public key of a first key pair;

preventing the decryption of said encrypted digital data by preventing the use of the corresponding private key of said first key pair; and

replacing said first key pair with a second key pair for encrypting and decrypting further digital data.

180. (New) The method according to claim 179, wherein said preventing step comprises revoking or deleting said private key.

181. (New) The method according to claim 179, wherein said encrypting step is performed by a first party of said system, the corresponding decryption is performed by a second party of said system, said preventing and said replacing steps are at least one of controlled, initiated and enforced by means of said system, whereby said method further comprises a step of providing said encrypted digital data to said second party via a network and a step of storing said encrypted digital data or a respective copy thereof by said second party.

182. (New) The method according to claim 181, wherein said network is the Internet.

183. (New) The method according to claim 179, wherein said preventing step is automatically performed according to a first schedule and said replacing step is automatically performed according to a second schedule.

184.   (New) The method according claim 181, whereby said first and said second schedule are independent from one another and specified by either said system or said first party.

185.   (New) The method according to claim 183, wherein at least one of said first and said second schedule comprises respectively a first and a second time span, whereby respectively said preventing step and said replacing step are performed after said first and said second time span have expired, and whereby respectively said first and/or said second time span starts with one of the following:

said encrypting step;

said provision of said encrypted data to said second party;

the generation or distribution of said first or second key pair; or

a predetermined time after the respectively other first or second time span has started.

186.   (New) The method according to claim 179, wherein at least one of said first and said second key pair is generated, distributed or provided by dedicated means of said system.

187.   (New) The method according to claim 179, wherein more than one first key pair is used in concurrent or overlapping time periods and/or replaced by more than one second key pairs.

188.   (New) The method according to claim 187, wherein each of said more than one first key pairs is respectively used for at least one of different kinds of digital data, different groups of said first parties and different groups of said second parties, whereby said preventing step and said replacing step are selectively and independently applied to each of said more than one first key pair to selectively control the access to said encrypted digital data.

189. (New) The method according to claim 179, further comprising a step of preventing the use of the public key of said first key pair by controlled deleting or revoking said public key.

190. (New) The method according to claim 181, wherein said step of preventing the use of said public key is at least one of initiated, controlled and enforced by means of said system or said first party, whereby said method is used to provide for said second user to still access said digital data by said decryption process using said private key after said step of preventing the use of said public key.

191. (New) The method according to claim 179, wherein said method is used for at least one of:

undermining fraud to said previously encrypted data;

said digital data that is to be deleted after a specified or predetermined time frame, whereby additionally possible backup copies and/or log information of said encrypted digital data are also to be deleted;

ensuring that a possible disclosure of said private key of said first key pair does not compromise the security and privacy of said encrypted digital data.

192. (New) A method for controlling the distribution of digital data in a public key system, the method comprising:

computing encrypted digital data by encrypting said digital data using a public key of a first key pair;

decrypting said encrypted digital data using the corresponding private key of said first key pair;

preventing said encryption step for further digital data by preventing the use of said public key; and

replacing said first key pair with a second key pair for encrypting and decrypting further digital data.

193. (New) The method according to claim 192, wherein said encrypting step is performed by a first party of said system, the corresponding decrypting step is performed by a second party of said system, said preventing and replacing steps are at least one of controlled, initiated and enforced by dedicated means of said system, whereby said method further comprises a step of providing said encrypted digital data to said second party via a network.

194. (New) The method according to claim 192, wherein said preventing step comprises revoking or deleting said public key.

195. (New) The method according to claim 192, further comprising a step of controlled deleting or revoking said private key of said first key pair by means of said system.

196. (New) A method for controlling the distribution of digital data in a public key system, the method comprising:

computing a digital signature on said digital data using a private key of a first key pair according to a first digital signature scheme;

verifying said digital signature using the corresponding public key of said first key pair according to said first digital signature scheme;

preventing said computing step for further digital data by preventing the use of said private key; and

replacing said first key pair with a second key pair for computing and verifying digital signatures on further digital data.

197. (New) The method according to claim 196, wherein said computing step is performed by a first party of said system, the corresponding verifying step is performed by a second party of said system, said preventing and replacing steps are at least one of controlled, initiated and enforced by dedicated means of said system, whereby said

method further comprises a step of providing said digital signature and said digital data to said second party via a network.

198. (New) The method according to claim 196, wherein said second party rejects said provided digital data if said step of verifying said digital signatures fails, or wherein said second party is only able to or allowed to use and access said provided digital data if said verifying step succeeds.

199. (New) The method according to claim 196, wherein said method further comprises a step of encrypting said digital data in connection with said computing step and a step of decrypting said digital data after a successful verifying step.

200. (New) The method according to claim 196, wherein said preventing step comprises revoking or deleting said private key.

201. (New) The method according to claim 193, wherein said network is the Internet.

202. (New) The method according to claim 192, wherein said preventing step is automatically performed according to a first schedule and said replacing step is automatically performed according to a second schedule.

203. (New) The method according to claim 202, whereby said first and said second schedule are independent from another and specified by either said system or said first party.

204. (New) The method according to claim 192, wherein at least one of said first and said second schedule comprise respectively a first and a second time span, whereby respectively said preventing step and said replacing step are performed after said first and

said second time span have expired, and whereby respectively said first and said second time span starts with one of the following:

> said computing step;
>
> said step of providing to said second party;
>
> the generation or distribution of said first or second key pair; or
>
> a predetermined time after the respectively other first or second time span has started.

205. (New) The method according to claim 192, wherein at least one of said first and said second key pair is generated, distributed or provided by said system.

206. (New) The method according to claim 192, wherein more than one first key pair is used in concurrent or overlapping time periods.

207. (New) The method according to claim 206, wherein each of said more than one first key pair is respectively used for at least one of different kinds of digital data, different groups of said first parties and different groups of said second parties, whereby said preventing step and said replacing step are selectively and independently applied to each of said more than one first key pair to selectively control the secure distribution to said digital data.

208. (New) The method according to claim 192, whereby said method is used to control that no additional digital data can be added to a pool of digital data, whereby previous digital data associated with said pool can still be distributed, used or accessed, whereby different pools of digital data are established by different key pairs.

209. (New) A computer-readable storage medium having a computer program for controlling a plurality of client terminals of a public key system to participate in and perform operations according to a method as specified by claim 192.

210.   (New) A computer-readable storage medium having a computer program for controlling a server of a public key system to participate in and perform operations according to a method as specified by claim 192.

211.   (New) A method for providing a layered asymmetric encryption of digital data in a data distribution system, said method comprising the steps of:
encrypting said digital data using a first key in a first encryption layer;
encrypting said first key using a second key in said first encryption layer;
encrypting said encrypted first key using a third key in a second encryption layer;
providing said encrypted data and said encrypted first key;
decrypting said encrypted first key according to said second encryption layer; and
decrypting said encrypted first key according to said first encryption layer; and
decrypting said encrypted digital data according to said first encryption layer.

212.   (New) The method according to claim 211, wherein said encrypting step of said digital data is performed by a first party of said system, whereby said first key is a symmetric key,
said encrypting step of said first key in said first encryption layer is performed by said first party, whereby said second key is the public key of a first public key pair,
said encrypting step of said encrypted first key in said second encryption layer is performed by said first party or a second party of said system, whereby said third key is the public key of a second public key pair,
said providing step provides said encrypted data and said encrypted first key to a third party of said system by means of a network,
said decrypting step of said encrypted first key according to said second encryption layer is performed by said third party using the private key of said second public key pair,

said decrypting step of said encrypted first key according to said first encryption layer is performed by said third party or a fourth party of said system using the private key of said first public key pair,

said decrypting step of said encrypted digital data is performed by said third or fourth party using said decrypted first key.

213. (New) The method according to claim 211, further comprising

a step of encrypting said encrypted first key using a fourth key in a third encryption layer after said encrypting in said second encryption layer, and

a step of decrypting said encrypted first key according to said third encryption layer before said decrypting step according to said second encryption layer.

214. (New) The method according to claim 213, wherein said step of encrypting said first key using said fourth key is performed by one of said first party, said second party or a fifth party, whereby said fourth key is the public key of a third public key pair, and said step of decrypting according to said third encryption layer is performed by one of said third party, said fourth party or a sixth party of said system using the private key of said third public key pair.

215. (New) The method according to claim 211, wherein one or more of said encrypting steps of said first key further comprising encrypting said digital data using the encryption key of the respective encryption layer.

216. (New) The method according to claim 212, wherein one or more of said encryption steps of said encrypted first key comprise:

encrypting said first key using a further symmetric key,

encrypting said further symmetric key using the public key of the respective public key pair of the encryption layer of said one or more encryption step, and

associating said encrypted further symmetric key with said encrypted first key, whereby said encrypted further symmetric key is treated in the same manner as said first key by any following encryption layer, whereby said following encryption layer regards both encrypted keys either as one key information part or as two separate encrypted keys; and

wherein the corresponding decrypting step of said encryption steps comprise:

decrypting said encrypted further symmetric key using the private key of the public key pair of said respective encryption layer,

decrypting said encrypted first key using said decrypted further symmetric key.

217.   (New) A method for controlling the distribution path of digital data from a sender to a recipient via a network, whereby said network comprises a plurality of connected network nodes, said method comprising the steps of:

(a)   encrypting said digital data using a first key in a first encryption layer;

(b)   encrypting said first key using a second key in said first encryption layer, whereby said second key is a public key associated with said recipient of said digital data;

(c)   encrypting said encrypted first key using a third key in a second encryption layer, whereby said third key is a public key associated with a first network node said digital data is defined to pass along a distribution path through said network to said recipient;

(d)   providing said encrypted data and said encrypted first key to said first network node;

(e)   decrypting said encrypted first key at said first network node according to said second encryption layer using the corresponding private key to said public key of said first network node;

(f)   providing said encrypted data and said encrypted first key to said recipient;

(g)   decrypting said encrypted first key according to said first encryption layer using the corresponding private key of said public key of said recipient; and

(h)   decrypting said encrypted digital data according to said first encryption layer using said decrypted first key.

218.   (New) The method according to claim 217, wherein said encrypting step c) is performed by said sender or a third network node the message comprised of said encrypted data and said encrypted first key has previously passed.

219.   (New) The method according to claim 217, further comprising the steps of

encrypting said encrypted first key using a fourth key in a third encryption layer, whereby said fourth key is a public key associated with a second network node said digital data is defined to pass along a distribution path through said network to said recipient;

providing said encrypted data and said encrypted first key to said second network node; and

decrypting said encrypted first key at said second network node according to said third encryption layer using the corresponding private key of said public key of said second network node.

220.   (New) The method according to claim 219, wherein said encrypting step is performed by one of said sender, said first network node, or a third network node said message comprised of said encrypted data and said encrypted first key has previously passed.

221. (New) The method according to claim 217, further comprising the following steps that are performed by each network node after having received said encrypted digital data and said encrypted first key:

establishing whether said received encrypted first key is to be decrypted by said network node according to a specific encryption layer;

if said network node has to decrypt said encrypted first key, decrypting said encrypted first key according to said specific encryption layer using the respective private key;

establishing the next network node of said network including said recipient, said encrypted digital data and said encrypted first key have to be provided to by said network node;

establishing whether said encrypted first key has to be encrypted in at least one further encryption layer using a public key associated with said next network node and/or a public key of a further network node;

if said encrypted first key has to be encrypted, obtaining said public key and encrypting said encrypted first key according to said further encryption layer using said public key according to said further encryption layer;

222. (New) The method according to claim 217, wherein said sender and/or a network node transmitting said encrypted data and said encrypted first key specifies at least one network node of said network including said recipient, said encrypted data and said encrypted first key have to pass when being transmitted to said recipient.

223. (New) The method according to claim 222, wherein said specifying is at least comprised of encrypting said encrypted first key according to an encryption layer using a public key of said specified network node.

224. (New) A computer-readable storage medium having a computer program for controlling a plurality of network nodes of a network, said computer program causing a

network node to perform the steps of claim 221 after having received a message comprised of an encrypted digital data part and an encrypted first key part.

225.   (New) The computer program according to claim 224, further causing said network nodes to perform the step of specifying at least one network node of said network including said recipient, said encrypted data and said encrypted first key have to pass when being transmitted to said recipient, whereby said specifying step at least comprises encrypting said encrypted first key according to an encryption layer using a public key of said specified network node.

226.   (New) A computer-readable storage medium having a computer program for controlling a plurality of client terminals of a public key system to participate in and perform operations according to a method as specified by claim 211.

227.   (New) A method for controlling the distribution of digital data in a public key system using digital signatures on said digital data, said method comprising the steps of:

computing a hash value of said digital data by a sender;

computing a first digital signature by said sender by encrypting said hash value according to a first digital signature scheme using a first private key of a first public key pair;

computing a second digital signature by encrypting said first digital signature according to a second digital signature scheme using a second private key of a second public key pair;

providing said second digital signature and said digital data to a recipient of said digital data;

computing a first verification value of said second digital signature according to said second digital signature scheme using the public key of said second public key pair;

computing a second verification value of said first verification value according to said first digital signature scheme using the public key of said first public key pair;

obtaining a hash value of said digital data;

comparing said obtained hash value and said second verification value; and

if said comparing step shows different values, establishing that the data distribution process to said recipient deviates from the intended process flow.

228.   (New) The method according to claim 227, further comprising the step of:

obtaining said first digital signature in either said providing step together with said provided digital data and said provided second digital signature or in a further providing step;

comparing said obtained first digital signature and said computed first verification value;

if said comparing step shows different values, establishing that the data distribution process to said recipient deviates from the intended process flow.

229.   (New) The method according to claim 227, wherein said obtaining step of said hash value comprises at least one of

computing said hash value from said provided digital data in the same manner as said first computing step of said hash value performed by said sender, or

obtaining said hash value in said providing step together with said provided digital data and said provided second digital signature.

230.   (New) The method according to claim 227, wherein said step of computing a second digital signature further comprises the step of:

computing a third digital signature by encrypting said first digital signature according to a third digital signature scheme using a third private key of a third public

key pair to replace said first digital signature prior to said computing of said second digital signature; and

wherein said step of computing a second verification value further comprises the step of:

computing a third verification value of said first verification value according to said third digital signature scheme using the public key of said third public key pair to replace said first verification value prior to said computing of said second verification value.

231. (New) The method according to claim 230, further comprising the steps of:

obtaining said third digital signature in one of said providing step together with said provided digital data and said provided second digital signature, or a further providing step;

comparing said obtained third digital signature and said computed first verification value prior to said step of computing a second verification value;

if said comparing step shows different values, establishing that the data distribution process to said recipient deviates from the intended process flow.

232. (New) The method according claim 227, wherein said digital is encrypted for said distribution process in the manner as defined by claim 211, whereby each of said computing steps of said digital signatures and the respective computing steps of said verification values, the respective comparing and establishing steps are associated to and performed ion connection with one of said encryption layers.

233. (New) A method for controlling the distribution path of digital data from a sender to a recipient via a network, whereby said network comprises a plurality of connected network nodes, said method comprising the steps of claim 227, whereby at least one of said network nodes performs one of said steps of computing a digital signature.

234. (New) The method according to claim 233, whereby at least one of said network nodes performs said steps of computing a verification value, obtaining a hash value, comparing and establishing.

235. (New) The method according to claim 233, whereby at least one of said network nodes performs at least one group of the following steps, whereby each step is associated with one specific of said public key pairs:

    said step of computing a verification value,

    said step of obtaining a digital signature,

    said step of comparing said obtained digital signature and said computed verification value, and

    said establishing step.

236. (New) The method according to claim 217, further comprising the steps of

encrypting said encrypted first key using a fourth key in a third encryption layer, whereby said fourth key is a public key associated with a second network node said digital data is defined to pass along a distribution path through said network to said recipient;

providing said encrypted data and said encrypted first key to said second network node; and

decrypting said encrypted first key at said second network node according to said third encryption layer using the corresponding private key of said public key of said second network node.

237. (New) The method according to claim 227, wherein the signature schemes, each associated with one of said public key pairs, can be different from one another and are predetermined or specified by said system, said sender of said digital data, or another party within said system that provides said digital data to another party within said system.

238. (New) The method according to claim 233, further comprising the following steps that are performed by each network node after having received said digital data and said digital signature:

establishing whether said received digital signature has to be digitally signed by said network;

if said network node has to digitally sign said received digital signature, computing a further digital signature by encrypting said received digital signature according to a further digital signature scheme using a further private key of a further public key pair to replace said received digital signature prior to providing said digital data and said computed digital signature to a further network node or to said recipient;

establishing the next network node of said network including said recipient, said digital data and said computed digital signature have to be provided to by said network node.

239. (New) A computer-readable storage medium having a computer program for controlling a plurality of network nodes of a network, said computer program causing a network node to perform the steps of claim 238 after having received a message comprised of said digital data and said digital signature.

240. (New) A computer-readable storage medium having a computer program for controlling a plurality of client terminals of a public key system to participate in and perform operations according to a method as specified by claim 227.

241.   (New) A method for providing a secure communication for exchanging digital data in a client-server-system, said system comprises at least one server and a plurality of client terminals which are connected via a network, said method comprising the steps of:

encrypting digital data by a client terminal of said system using a previously obtained first hash value as key information in a symmetric encryption scheme;

providing said encrypting digital data and a previously obtained random token to a server of said system by said client terminal; whereby said first hash value is associated with said random token and serves as a shared secret between said server and said client terminal;

said server computing a second hash value of said provided random token and a fixed random value, whereby said fixed random value is a secret, private value in possession of said server and not disclosed to said plurality of client terminals; and

decrypting said encrypted digital data by said server using said second hash value as key information according to said symmetric encryption scheme.

242.   (New) The method according to claim 241, further comprising the steps of:

obtaining said random token prior to said encrypting step;

providing said random token to said server prior to said encrypting step;

computing said first hash value of said random token and said fixed random value by said server prior to said encrypting step; and

providing said first hash value to said client terminal prior to said encrypting step;

243.   (New) The method according to claim 242, wherein said steps of

obtaining said random token,

providing said random token,

computing said first hash value, and

providing said first hash value are performed as part of an initial registration process of said client terminal with said server, and wherein all remaining steps are performed as part of the secure data exchange transaction of said digital data.

244. (New) The method according to claim 242, wherein

said step of providing said random token further comprises a prior step of encrypting said random token according to an asymmetric encryption scheme; and

said step of computing said first hash value further comprises a prior step of decrypting said random token according to said asymmetric encryption scheme.

245. (New) The method according to claim 242, wherein

said step of providing said first hash value to said client terminal further comprises a prior step of encrypting first hash value according to an asymmetric encryption scheme; and

said client terminal further performs a step of decrypting the encrypted first hash value according to said respective asymmetric encryption scheme after having received said encrypted first hash value.

246. (New) The method according to claim 242, wherein said step of obtaining said random token comprises generating said random token at said client terminal.

247. (New) The method according to claim 242, wherein said steps of obtaining said random token and of providing said random token to said server are accomplished by a step of generating said random token at said server; and

said step of providing said first hash value further comprises providing said generated random token to said client terminal; whereby said random token is encrypted and decrypted in the same manner as said first hash value if

said first hash value is encrypted and decrypted in connection with said providing step.

248. (New) The method according to claim 242, wherein said server uses a plurality of different fixed random values, whereby all or some of said plurality of different fixed random values can be used successive, concurrent or overlapping time periods, and wherein each of said plurality of different fixed random values can be used for at least one of the following:

different groups of client terminals;

different registration times of client terminals with said server; or

different time periods or points in time for performing at least one of said steps of said method.

249. (New) The method according to claim 248, wherein said steps of obtaining said random token and of providing said random token to said server comprising a step of generating a part of said random token at said server; and

said step of providing said first hash value further comprising providing said generated random token to said client terminal; whereby said random token is encrypted and decrypted in the same manner as said first hash value if said first hash value is encrypted and decrypted in connection with said providing step; and wherein

said server further performing the step of:

choosing a particular of said plurality of different fixed random values prior to said step of computing said first hash value;

associating said particular of said plurality of different fixed random values with said generated part of said random token;

establishing said particular of said plurality of different fixed random values prior to said step of computing said second hash value by determining said generated part from said provided random token and

subsequently identifying the associated particular fixed random value thereof.

250. (New) The method according to claim 248, further comprising the steps of:

choosing a particular of said plurality of different fixed random values prior to said step of computing said new first hash value;

establishing said particular of said plurality of different fixed random values prior to said step of computing said second hash value by successively testing each of said different fixed random values whether it produces a valid result in said following step of decrypting said encrypted digital data by said server.

251. (New) The method according to claim 241, further comprising the steps of:

encrypting digital data of a reply message to said client terminal by said server using said second hash value as key information according to said symmetric encryption scheme;

providing said encrypted digital data of said reply message to said client terminal; and

decrypting said encrypted digital data of said reply message by said client terminal using said first hash value as key information according to said symmetric encryption scheme.

252. (New) The method according to claim 242, wherein said steps of

obtaining said random token,

providing said random token,

computing said first hash value, and

providing said first hash value are performed as new registration process of a client terminal with said server, if said fixed random value in possession of said server and used for said computing steps is replaced with a new fixed random value.

253. (New) The method according to claim 248, wherein said plurality of different fixed random values are replaced independently from one each other, and wherein said method provides for selectively requiring a specific group of users that is associated with a specific one of said plurality of fixed random values to register again with said server.

254. (New) The method according to claim 241, wherein said client terminal remains anonymous for said server and wherein said server is not required to store record information on said client terminals containing their associated tokens, their associated hash values that are used as key information in the respective symmetric encryption scheme, other shared secrets previously established between said server and said client terminals, or identifiers of said client terminals in order to establish one of: said associated token, said associated hash value or said shared secret.

255. (New) A system for providing a secure communication for exchanging digital data, said system comprising at least one server and a plurality of client terminals which are connected via a network, said client terminals comprising:

    means for encrypting digital data using a previously obtained first hash value as key information in a symmetric encryption scheme;

    means for providing said encrypting digital data and a previously obtained random token to a server of said system; whereby said first hash value is associated with said random token and serves as a shared secret between said server and said client terminal;

said at least one server comprising:

    means for computing a second hash value of said provided random token and a fixed random value, whereby said fixed random value is a secret, private value in possession of said server and not disclosed to said plurality of client terminals; and

means for decrypting said encrypted digital data using said second hash value as key information according to said symmetric encryption scheme;

256. (New) The system according to claim 255, wherein said client terminals further comprising:

means for obtaining said random token prior to the encryption of said digital data;

means for providing said random token to said server prior to said encryption of said digital data; and

wherein said at least one server further comprising:

means for computing said first hash value of said random token and said fixed random value prior to said encryption of said digital data; and

means for providing said first hash value to said client terminal prior to said encryption of said digital data.

257. (New) The system according to claim 255, wherein said server means for providing said first hash value further comprises means for providing said partially generated random token to said client terminal; whereby said means provides further for said random token to be encrypted in the same manner as said first hash value if said first hash value is encrypted and decrypted in connection with said provision; and wherein

said server further comprising:

means for partially generating said random token;

means for choosing a particular of a plurality of different fixed random values prior to said computing of said first hash value;

means for associating said particular of said plurality of different fixed random values with said partially generated random token;

means for establishing said particular of said plurality of different fixed random values prior to said step of computing said second hash value by establishing said partially generated random token from said

provided random token and subsequently identifying the associated fixed random value thereof.

258. (New) The system according to claim 255, wherein said server further comprising:

means for encrypting digital data of a reply message to said client terminal using said second hash value as key information according to said symmetric encryption scheme; and

means for providing said encrypted digital data of said reply message to said client terminal; and wherein

said client terminal further comprising:

means for decrypting said encrypted digital data of said reply message using said first hash value as key information according to said symmetric encryption scheme.

259. (New) A computer-readable storage medium having a computer program for controlling a plurality of client terminals to participate in and perform operations according to a method as specified by claim 241.

260. (New) A computer-readable storage medium having a computer program for controlling a server to participate in and perform operations according to a method as specified by claim 241.

261. (New) The method according to claim 241, further comprising a step of replacing said random token with a new random token to be used in the same manner as the original random token.

262. (New) The method according to claim 261, further comprising:

a step of generating said new random token by said server;

a step of computing a new first hash value of said new random token and said fixed random value by said server;

a step of encrypting said new first hash value by said server using said second hash value as key information according to said symmetric encryption scheme;

a step of providing said encrypted new first hash value to said client terminal together with or in connection with a reply message of said server to said client terminal;

a step of decrypting said encrypted new first hash value by said client terminal using said original first hash value;

a step of obtaining said new random token by said client terminal; and

a step of replacing said original random token at said client terminal with said new random token and replacing said original first hash value with said new first hash value at said client terminal; whereby said new random token and said new first hash value can be used in the same manner and applied to the steps of said method as described for the respective original random token and first hash value.

263.   (New) The method according to claim 262, wherein said step of generating said new random token by said server comprises using a predetermined part of the message provided by said step of providing said encrypting digital data and said previously obtained random token to generate said new random token, whereby said predetermined part is one or more of the following:

a predetermined part of said decrypted digital data,

a predetermined part of said encrypted digital data,

a hash value performed on at least said predetermined part or said complete decrypted digital data, or

a hash value performed on at least said predetermined part or said complete encrypted digital data.

264. (New) The method according to claim 263, wherein said step of obtaining said new random token by said client terminal comprises a step of generating said new random token by said client terminal using said predetermined part of the same message in the same manner as performed by said server in said first step of generating said new random token.

265. (New) The method according to claim 262, wherein said step of generating said new random token by said server is independent of any message or data provided by said client terminal to said server.

266. (New) The method according to claim 262, wherein said step of obtaining said new random token comprises a step of providing said new random token to said client terminal, whereby said new random token is encrypted and decrypted in the same manner as or together with said new first hash value prior and after said providing step.

267. (New) The method according to claim 263, wherein said step of generating said new random token by said server further comprises generating a part of said new random token at said server independent of said provided message, said method further comprising the steps of:

   choosing a particular of said plurality of different fixed random values prior to said step of computing said new first hash value;

   associating said particular of said plurality of different fixed random values with said generated part of said new random token; and

   establishing said particular of said plurality of different fixed random values prior to said step of computing said second hash value by determining said generated part of said provided random token and subsequently identifying the associated particular fixed random value thereof.

268. (New) The method according to claim 263, further comprising the steps of:

choosing a particular of said plurality of different fixed random values by said server prior to said step of computing said new first hash value;

establishing said particular of said plurality of different fixed random values by said server prior to said step of computing said second hash value by successively testing each of said different fixed random values whether it produces a valid result in said following step of decrypting said encrypted digital data by said server.

269. (New) The method according to claim 268, wherein said step of establishing depends on a timed schedule for said successively testing accounting for at least one of said plurality of different fixed random values.

270. (New) The method according to claim 261, wherein a new random token is generated, encrypted, provided, decrypted and replaced for at least one of the following:

for each communication and data exchange transaction process between said client terminal and said server;

for a predetermined number of said communications and data exchange transactions;

upon request of a user associated with said client terminal; and

upon request of said server.

217. (New) The system according to claim 255, wherein said server further comprising:

means for generating a new random token;

means for computing a new first hash value of said new random token and a fixed random value; and

means for encrypting said new first hash value using said second hash value as key information according to said symmetric encryption scheme; and

wherein said system further comprising:

means for providing said encrypted new first hash value to said client terminal together with or in connection with a reply message of said server to said client terminal; and

wherein said client terminal further comprising:

means for decrypting said encrypted new first hash value using said original first hash value;

means for obtaining said new random token; and

means for replacing said original random token at said client terminal with said new random token and replacing said original first hash value with said new first hash value at said client terminal; whereby said new random token and said new first hash value can be used in the same manner and applied to the means of said system as specified in connection with the respective original random token and first hash value.

272.   (New) A computer-readable storage medium having a computer program for controlling a plurality of client terminals to participate in and perform operations according to a method as specified by claim 261.

273.   (New) A computer-readable storage medium having a computer program for controlling a server to participate in and perform operations according to a method as specified by claim 261.